СИСТЕМА ОПОВЕЩЕНИЯ О НЕСАНКЦИОНИРОВАННОМ ДОСТУПЕ К СЕТЕВОМУ ОБОРУДОВАНИЮ

П.С. Цикота, Е.С. Чиркин
Тамбовский государственный университет имени Г.Р. Державина, Тамбов, Россия

На сегодняшний день, в эпоху развития компаний интернет-провайдеров, работающих с локальными сетями, построенными на протоколе Fast Ethernet, существует актуальная угроза несанкционированного доступа к сетевому оборудованию, которая проявляется в краже оборудования, вандализме (нарушение работы сети путем повреждения проводов и оборудования), несанкционированном подключении с разным умыслом. Для интернет-провайдеров данная угроза усугубляется тем, что сетевое оборудование (коммутаторы), расположено, как правило, на технических этажах зданий, не принадлежащих компании. Следует заметить, что угрозы исходят не только от потенциального нарушителя в виде обычного человека или недобросовестного сотрудника компании, но и от конкурирующей фирмы [1; 3].

По подсчетам специалистов, интернет-провайдеры терпят значительные убытки от краж активного оборудования и кабеля типа витая пара. Каждый случай кражи провода обходится провайдеру в среднем в 25–30 тысяч рублей. В эту сумму входит восстановление кабеля, оплата работы монтажника, компенсация клиентам отсутствия соединения на время устранения неисправности и т. д. Кража активного оборудования приводит к убыткам порядка 50–70 тысяч рублей, в зависимости от количества абонентов, подключенных к данному оборудованию. В основном, кражей занимаются лица, которые продают оборудование и медные провода, входящие в витую пару [2].

Для повышения защиты сетевого оборудования была разработана система оповещения о несанкционированном доступе, базирующаяся на сигнальном устройстве, коммутаторе и сервере с установленным программным обеспечением.

Сигнальное устройство выполнено на витой паре и герконе с двумя режимами переключения. В качестве обработчика тревожного сигнала и передатчика его по каналам связи (локальная сеть интернет-провай-дера) до сервера используется собственно сетевое оборудование (коммутатор) с подключенным к нему сигнальным устройством, которое замыкает проводники витой пары, имитирующими подключение клиента. Используемое программное обеспечение на сервере: SNMP-менеджер и SMTP-сервер.

К достоинствам системы следует отнести следующее: дешевизна, легкость сборки и монтажа системы оповещения на предприятии с большой сетью. Компании не требуется прокладывать новые каналы связи системы сигнализации; монтаж и сборка сигнального устройства не требует специфических знаний и навыков, и его может провести практически любой штатный сотрудник (монтажник, сотрудник ремонтной службы). Настройку коммутационного оборудования можно провести как на месте расположения сетевого оборудования, так и удаленно. С этой задачей может справиться программист компании, системный администратор или сотрудник отдела защиты информации. Установку и настройку программного обеспечения на сервере также может провести штатный программист или системный администратор. Стоит отметить, что при использовании ОС Linux можно пользоваться стандартными утилитами, идущими с операционной системой.

Недостатками данной системы оповещения является отсутствие резервного канала связи и меньшая функциональность по сравнению с существующими специализированными средствами системы оповещения о несанкционированном доступе. Например, устройства NetPing TS v2, NetPing IO [4] и Ping 2 [5] оснащены термодатчиками, датчиками влажности, датчиками перепада напряжения в электрической сети и датчиками контроля звукового порога (датчик контроля «разбивающегося стекла»). Данные функциональности желательны, но не являются обязательными в конкретном случае размещения сетевого оборудования.

Таким образом, разработанная система будет полезна, в первую очередь, интернет-провайдерам, работающим с сетью на управляемых коммутаторах, которые не имеют возможности сделать значительные капиталовложения в установку

полнофункциональной системы сигнализации и оповещении о несанкционированном доступе к сетевому оборудованию.

Литература

1. Обзор случаев кражи сетевого оборудования. URL: http://www.spbit.ru/news/n61969/
2. Сообщение службы безопасности компании // Сайт компании InterZet. URL: http://www. interzet.ru/news/id343.html – 29.10.2010
3. Сотрудников домашней сети поймали на краже // Новостной портал Невского района города Санкт-Петербурга. URL: http://www. vposelok.ru/news/areanews/2740/
4. Устройства диагностики и мониторинга сетей серии PING2 // Официальный сайт производственной группы «Equicom». URL: http:// equicom.dp.ua/ping/ping2.htm
5. Устройство диагностики и мониторинга сетей NetPing TS v2 // Официальный сайт компании «Алентис Электроникс». URL: http://www. netping.ru